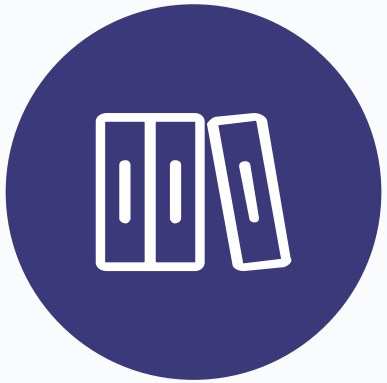


第8章 数据容灾备份

成都信息工程大学 白杨 副教授

2024年X月X日

第8章 数据容灾备份

本讲内容概要：

01 第一节—数据容灾备份概述

02 第二节—数据容灾备份技术

03 第三节—容灾备份系统的构建

01 1.1 容灾备份概念

容灾主要指的是面对灾难性事件时，系统能够保持其关键业务运行的能力。这通常涉及到在地理上分散的地点建立备份设施，以便在主站点发生故障时，能够迅速切换到备份站点，继续提供服务

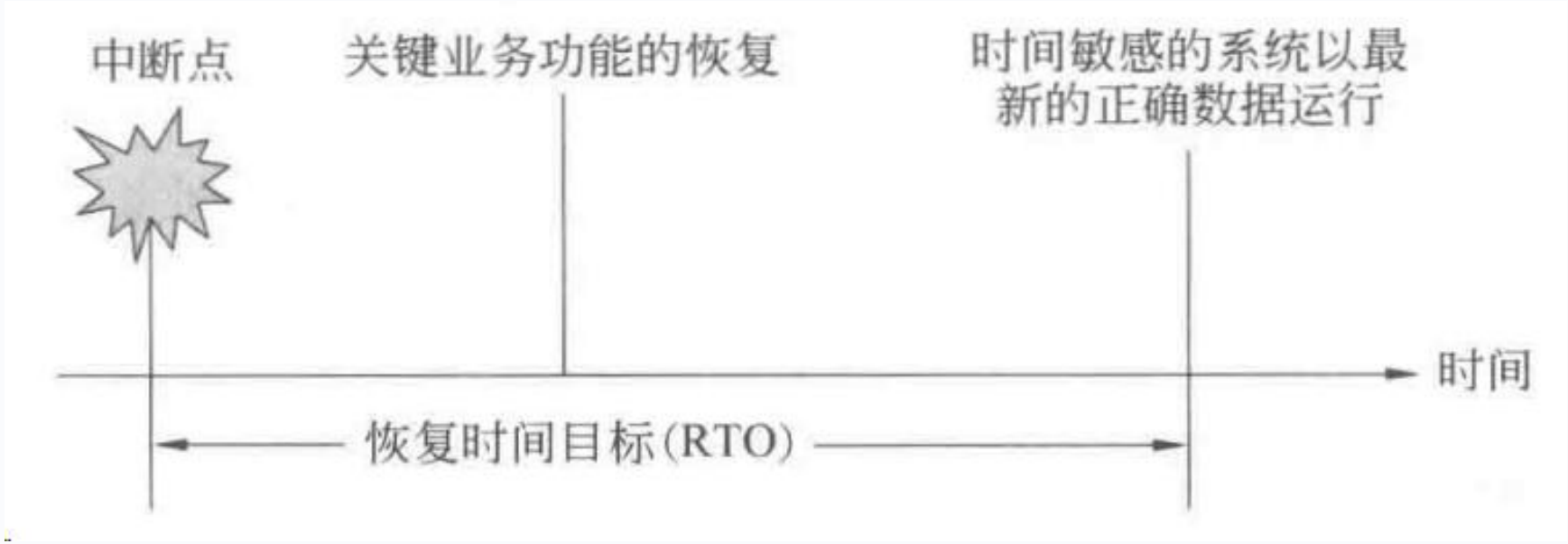
备份则是指将原始数据复制到另一个存储介质或位置，以防止数据丢失。备份可以是定期的、增量的或全量的，具体取决于业务需求和数据变化频率

容灾备份是为了应对可能发生的自然灾害、人为错误、硬件故障、软件漏洞或网络攻击等突发事件导致数据丢失或系统瘫痪的风险而采取的一系列预防性和恢复性措施。**核心目的**是确保数据的完整性、可用性和业务的连续性。

01 1.2 数据容灾指标

RTO

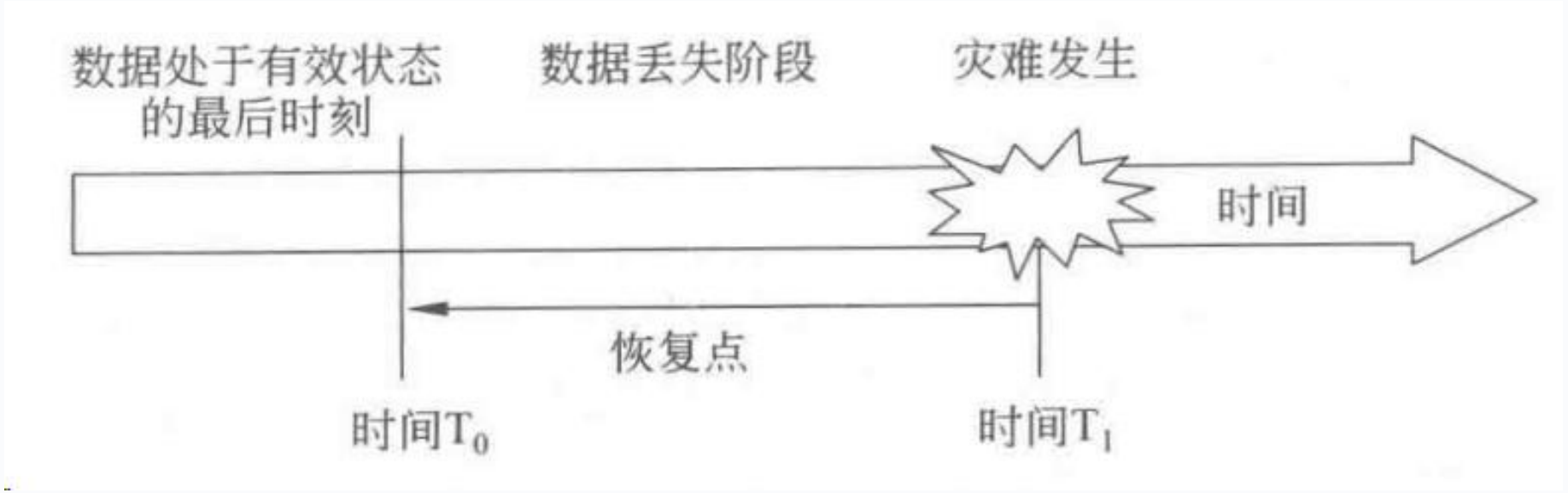
RTO（Recovery Time Objectives，即恢复时间目标）是指在灾难发生后，系统或应用程序需要恢复到正常运行状态的时间目标。它是确定业务恢复所需时间的最大时间限制。RTO通常是指从灾难发生时刻到系统恢复正常运行所需要的时间



01 1.2 数据容灾指标

RPO

RPO（Recovery Point Objectives，恢复点目标）是指灾难发生前的数据恢复目标。它是指最大允许数据丢失的时间。例如，如果灾难发生时刻是星期一早上9点，而RPO是1小时，那么系统必须能够恢复到星期一早上8点的状态。RPO通常是指为了确保在灾难发生时，数据恢复到最新的可接受状态所需的时间



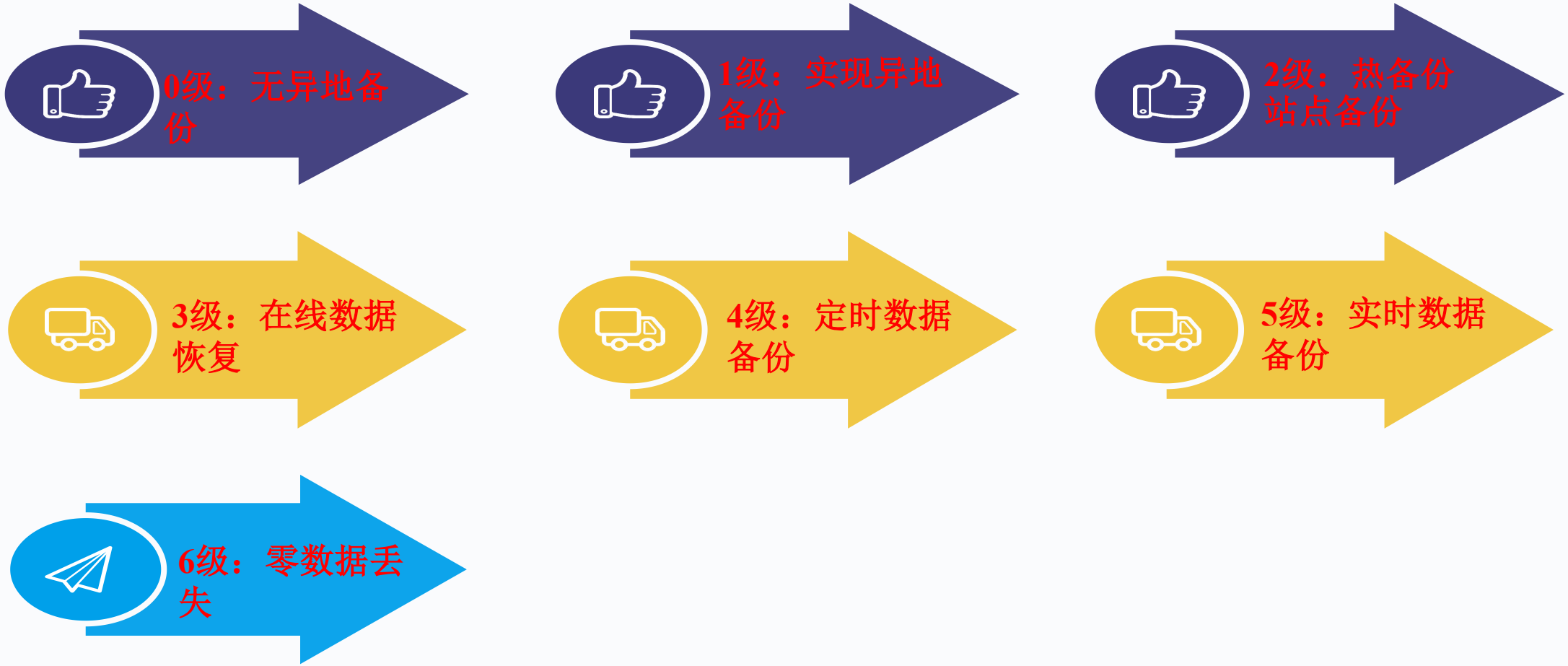
01 1.3 数据容灾级别

真正的容灾必须满足**三个要素**“3R”（Redundance、Remote、Replication）：

- 系统中的部件、数据都具有冗余性：即一个系统发生故障，另一个系统能够保持数据传送的顺畅
- 具有长距离性：灾害总是在一定范围内发生，因而充分长的距离才能够保证数据不会被一个灾害全部破坏
- 容灾系统要追求全方位的数据复制，也称为容灾的“3R”（Redundance、Remote、Replication）

01 1.3 数据容灾级别

国际标准SHARE 78 对容灾系统的定义有七个层次：从最简单的仅在本地进行磁带备份，到将备份的磁带存储在异地，再到建立应用系统实时切换的异地备份系统，恢复时间也可以从几天到小时级到分钟级、秒级或零数据丢失等



1.3 数据容灾级别

国际标准SHARE 78 对容灾系统的定义有七个层次：从最简单的仅在本地进行磁带备份，到将备份的磁带存储在异地，再到建立应用系统实时切换的异地备份系统，恢复时间也可以从几天到小时级到分钟级、秒级或零数据丢失等

2级：热备份　　站点备份

1级：实现异地备份

0级：无异地备份

5级：实时数据备份

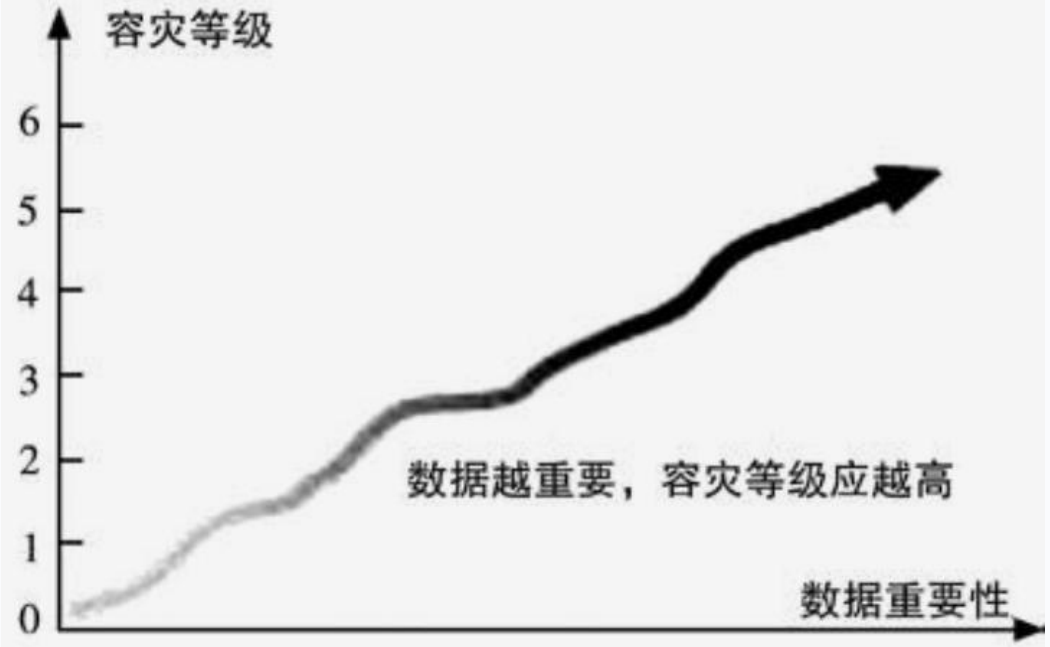
4级：定时数据备份

3级：在线数据恢复

6级：零数据丢失

01 1.4 数据容灾重要性

随着计算机技术的不断发展和信息化程度的不断提高，各企业逐步依赖于信息系统来支撑数据业务，海量数据带来的问题是如何确保数据的安全性和完整性。



为什么后果如此严重?

因为数据是计算机系统存在的原因和基础，数据往往是不可再生的。一旦发生数据丢失，企业就会陷入困境：客户资料、技术文件、财务账目等客户、交易、生产数据可能被破坏得面目全非。
因此，容灾系统对于某些关键业务而言也是必不可少的。人们谈及容灾备份往往是针对当生产系统，不能正常工作时，其业务可由容灾系统接替这些业务，继续进行正常的工作。

第1章 数据安全概述

本讲内容概要：

01 第一节—数据容灾备份概述

02 第二节—数据容灾备份技术

03 第三节—容灾备份系统的构建

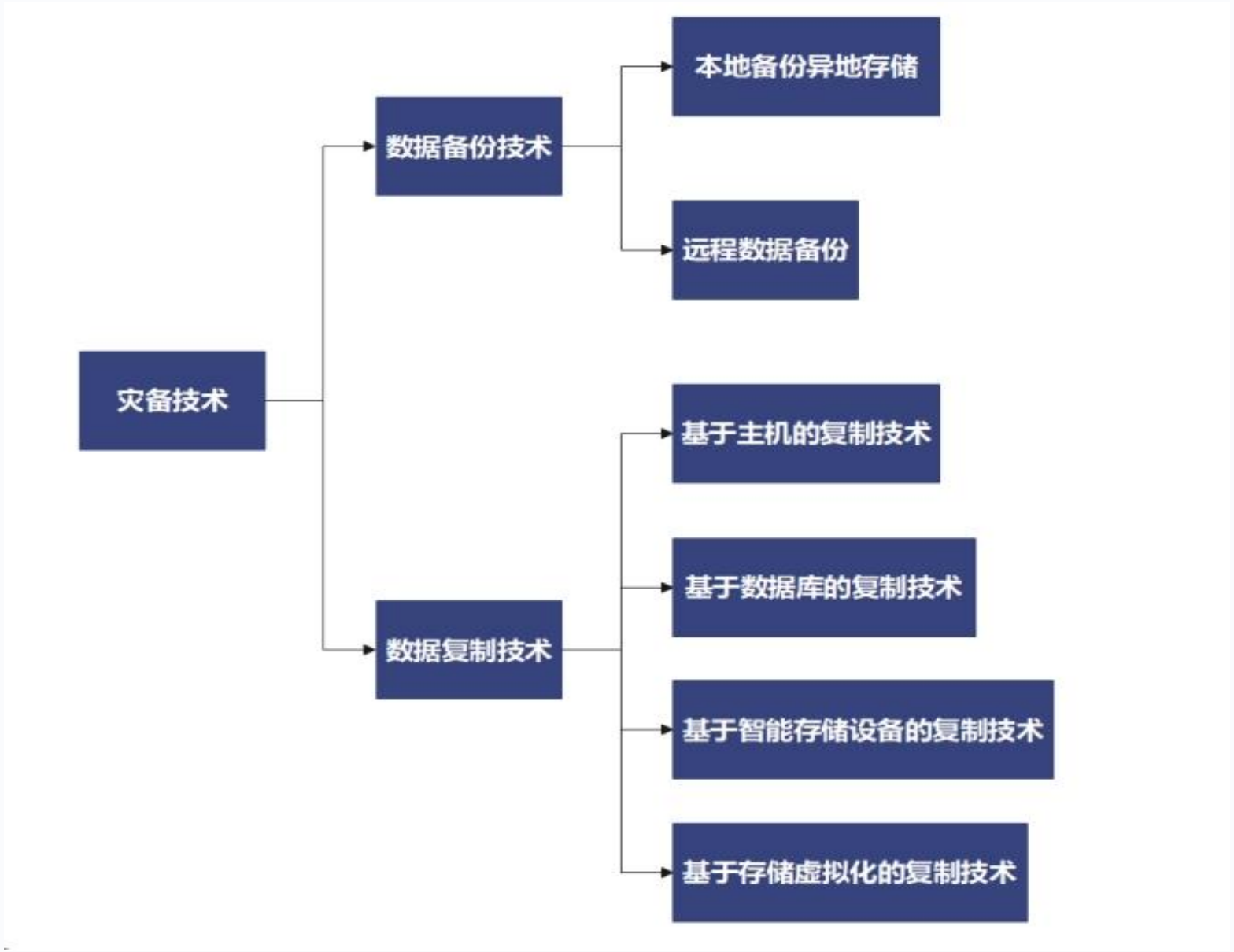
02 2.1 灾备技术介绍

灾备技术可以分为数据备份技术和数据复制技术两大类

数据备份技术主要是指通过定期或实时的方式，将重要数据备份到不同的存储介质或地点，以防止数据丢失或损坏。基于数据备份的灾备方案包括本地备份异地保存方案和远程数据备份方案

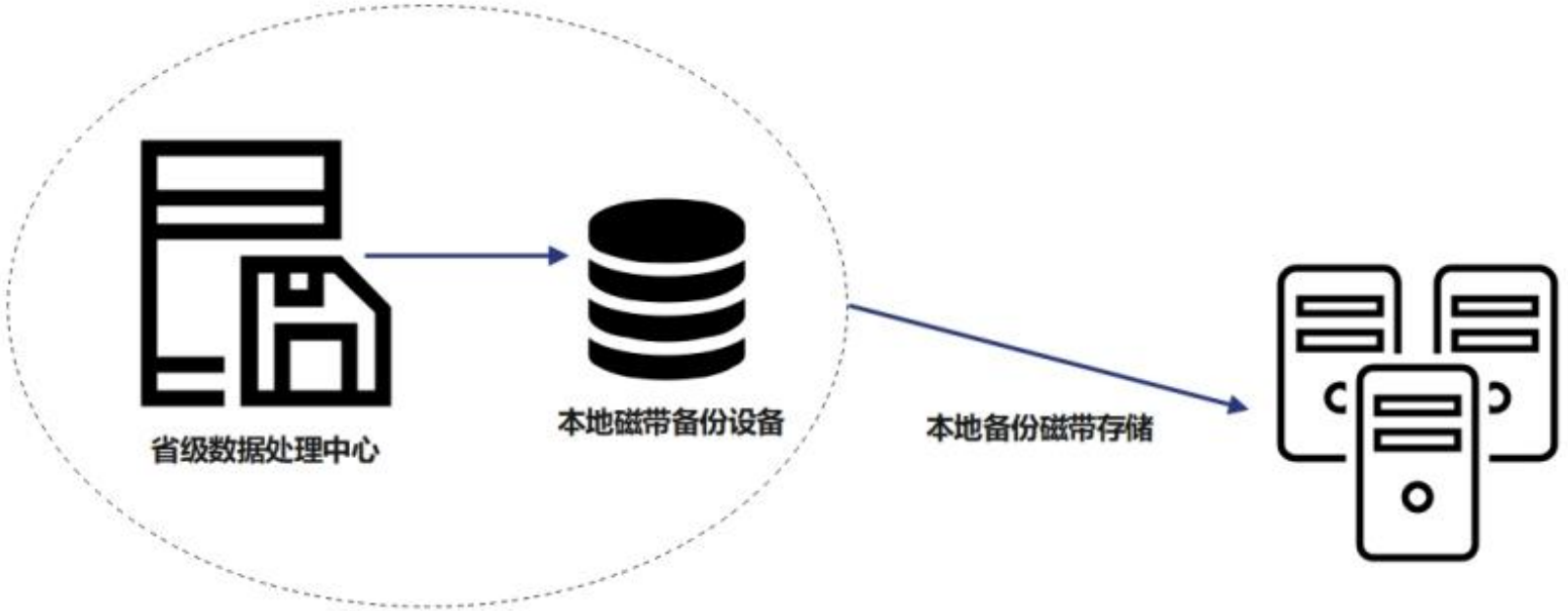
数据复制技术则强调在多个地点实时或定期地同步数据，以确保数据的一致性和可用性。这种技术可以即时反映数据的变化，并且能够在主数据中心出现故障时，迅速切换到备份数据中心，保证业务的连续性。数据复制技术又可分为基于智能存储设备的复制技术、基于主机的复制技术、基于数据库的复制技术和基于存储虚拟化的复制技术

02 2.1灾备技术介绍


灾备技术
数据备份技术
本地备份异地存储
远程数据备份
数据复制技术
基于主机的复制技术
基于数据库的复制技术
基于智能存储设备的复制技术
基于存储虚拟化的复制技术

02 2.1.1 本地备份异地存储

本地备份异地保存方案是一种将本地数据备份到远程地点的数据存储策略。此方案采用多种技术确保数据的完整性、可靠性和可用性。在本地，数据首先通过高效的数据备份软件进行全备份、增量备份或差异备份，备份两份，一份留在生产中心，一份将备份数据通过安全的网络连接传输到远程服务器或云存储中，用于灾难时的数据恢复



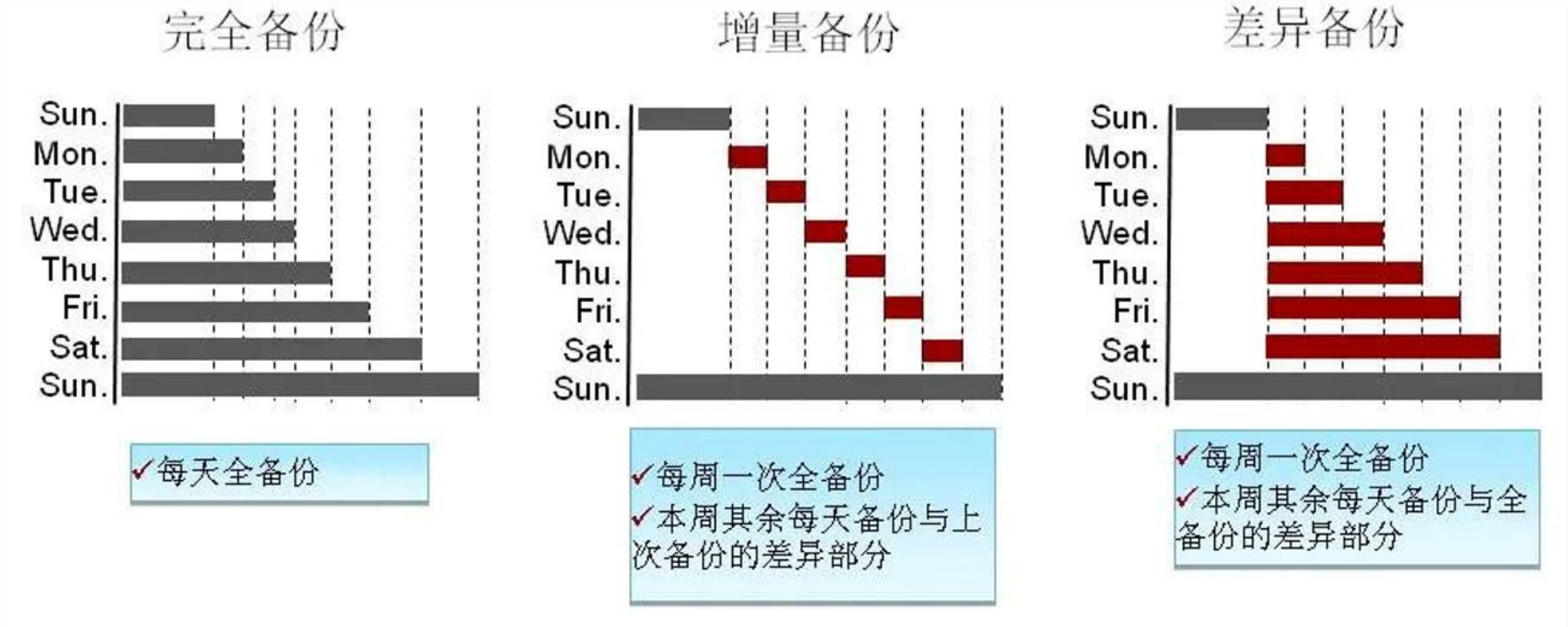
02 2.1.1 本地备份异地存储

实施本地备份异地保存方案需要以下资源配置：

- 本地备份设备：包括备份软件、备份服务器、磁带机、磁盘阵列等，用于实现本地数据的备份。
- 网络资源：需要稳定可靠的网络连接，确保备份数据能够安全、快速地传输到远程地点。
- 远程存储设备：包括远程服务器、云存储等，用于存储备份数据。
- 人员资源：需要专业的数据备份和恢复人员，负责方案的实施、监控和维护。

适用范围：本地备份异地保存方案适用于对数据安全性、可用性和连续性有较高要求的企业和组织，特别是那些数据量大、业务关键性强的行业，如金融、医疗、制造等

02 2.1.1 本地备份异地存储

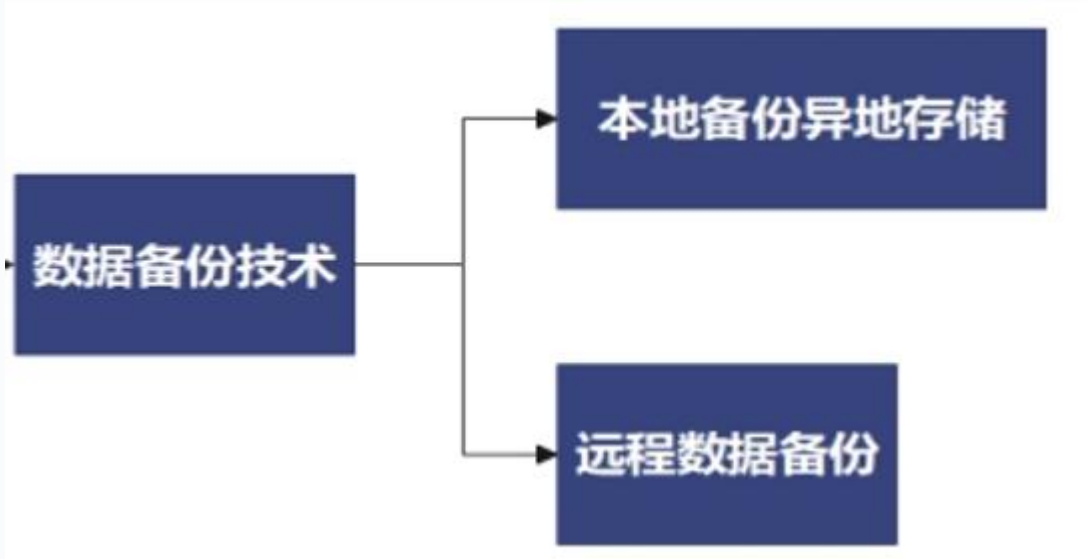


- **全备份：**是备份系统中所有的数据，所需时间最长但恢复时间最短，操作最方便，当数据量不大时最为可靠
- **增量备份：**只备份上次备份后有变化的数据，备份量小且时间短，但恢复时可能需要结合之前的备份数据
- **差异备份：**备份自上一次完全备份之后有变化的数据，恢复时只需结合最近一次的全备份和差异备份，兼具增量备份和全备份的优点

02 2.1.2 远程数据备份

远程数据备份方案与本地备份异地存放方案的核心差异在于数据传输方式。前者依赖生产中心与灾备中心之间的IP网络连接，实现数据的实时或定期远程备份；而后者则通过人工方式，将生产中心本地备份好的数据介质运送到灾备中心进行存储

这种方案确保了生产中心和灾备中心都存有生产数据的备份副本。当生产数据受损时，可以依赖生产中心的备份数据进行恢复；若生产中心遭遇灾难，灾备中心的备份数据则成为恢复的关键

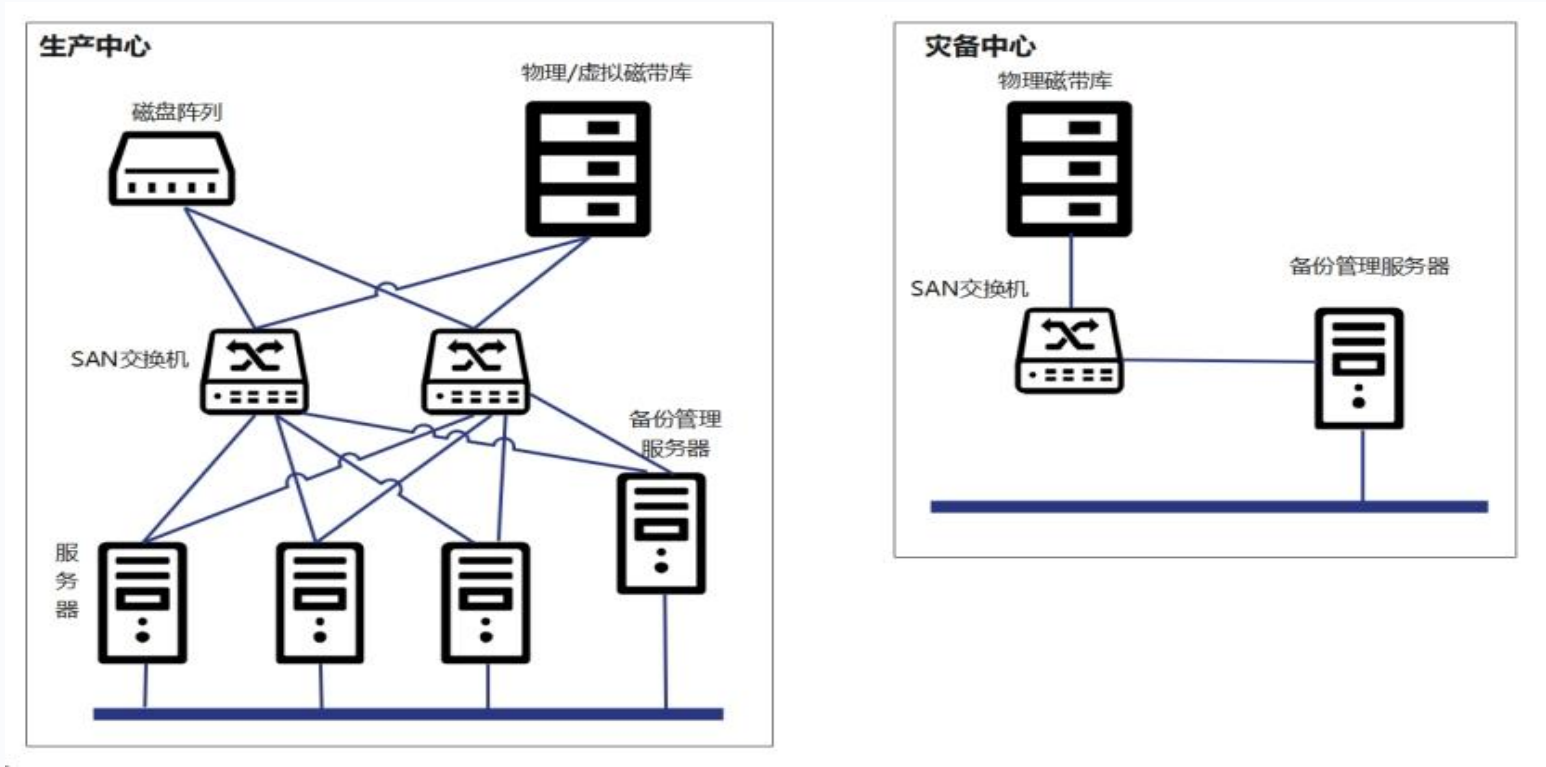


适用范围：本方案适用于生产数据较少且备份网络带宽较高的信息系统备份

02 2.1.2 远程数据备份

方案实现：

- 生产中心的备份管理服务器发出备份操作指令，将生产数据备份至本地的物理或虚拟带库，完成本地备份流程。
- 备份管理服务器通过IP网络对灾备中心的备份服务器进行作业管理和调度。通过广域网，生产中心物理或虚拟带库上的备份数据被传输至灾备中心的物理带库。
- 灾备中心的备份软件将数据传输至磁带，完成整个备份操作



02 2.2.1 基于智能存储设备的数据复制技术

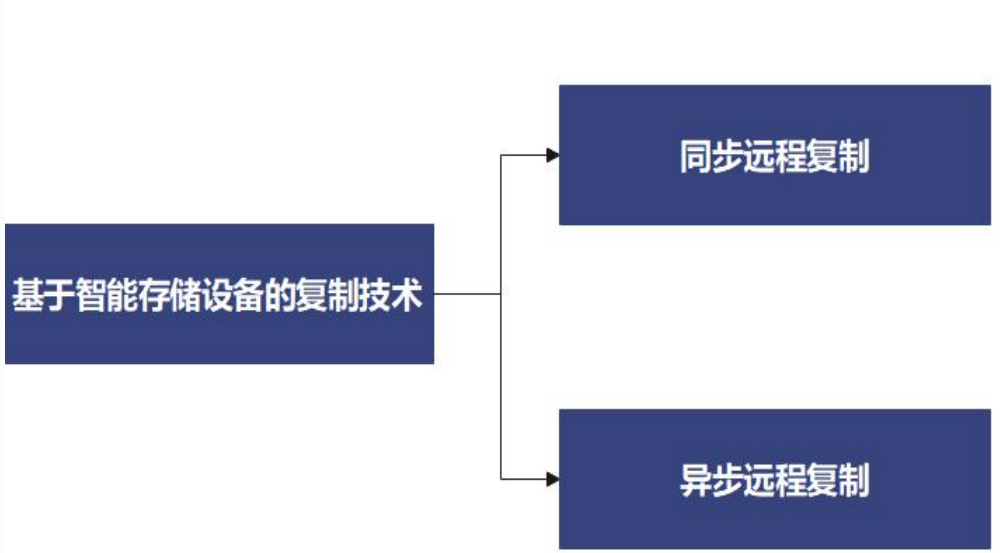
基于智能存储设备的数据复制技术，利用前沿的智能存储复制软件，通过光纤直连、IP网络等方式，在灾备中心与生产中心之间建立磁盘镜像连接，从而实现了数据的全天候远程实时复制

同步复制技术：

- 通过远程复制软件实现数据的即时同步，确保远程副本与本地数据一致性。
- 在主站点故障时，可以迅速切换至备份站点，保证业务连续性和数据完整性。
- 同步复制可能因数据往返传播而产生延时，更适合短距离传输

异步复制技术：

- 允许本地存储系统在远程复制完成前完成I/O操作，对性能影响小，适用于长距离传输
- 可能因远程数据复制失败而导致数据一致性问题。为解决此问题，通常采用延迟复制技术，通过在本地日志区复制数据后再更新远程副本，确保数据的一致性和完整性



02 2.2.1 基于智能存储设备的数据复制技术

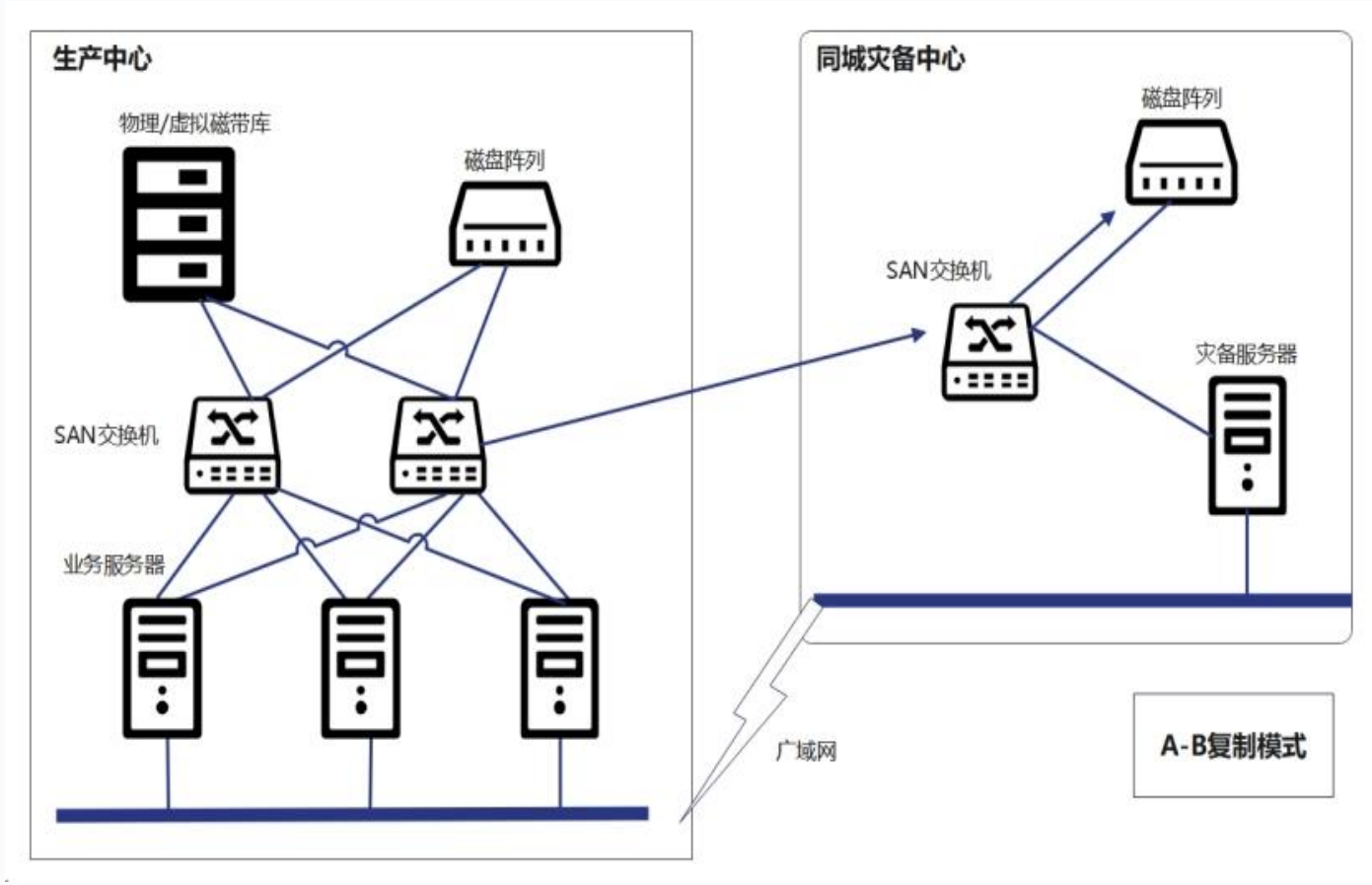
技术提供了三种相应的架构方案，即A-B模式、A-B-C模式和A-B/A-C模式

生产—同城复制模式（A—B模式）

在生产中心与同城灾备中心之间，采用的是基于磁盘阵列的同步复制模式

数据向远程镜像磁盘卷的写入过程如下：

- 系统接收来自生产中心主机的写I/O操作，这些数据会被写入生产中心本地磁盘阵列的缓存中
- 通过特定的链路，这些数据会被传输到同城灾备中心的磁盘阵列缓存中。一旦同城灾备中心的磁盘阵列成功接收到数据，它会向生产中心的磁盘阵列发送一个数据接收确认信号
- 系统会修改磁道表，以确保数据的完整性和一致性
- 系统会通知生产中心的主机，告知其I/O操作已经完成



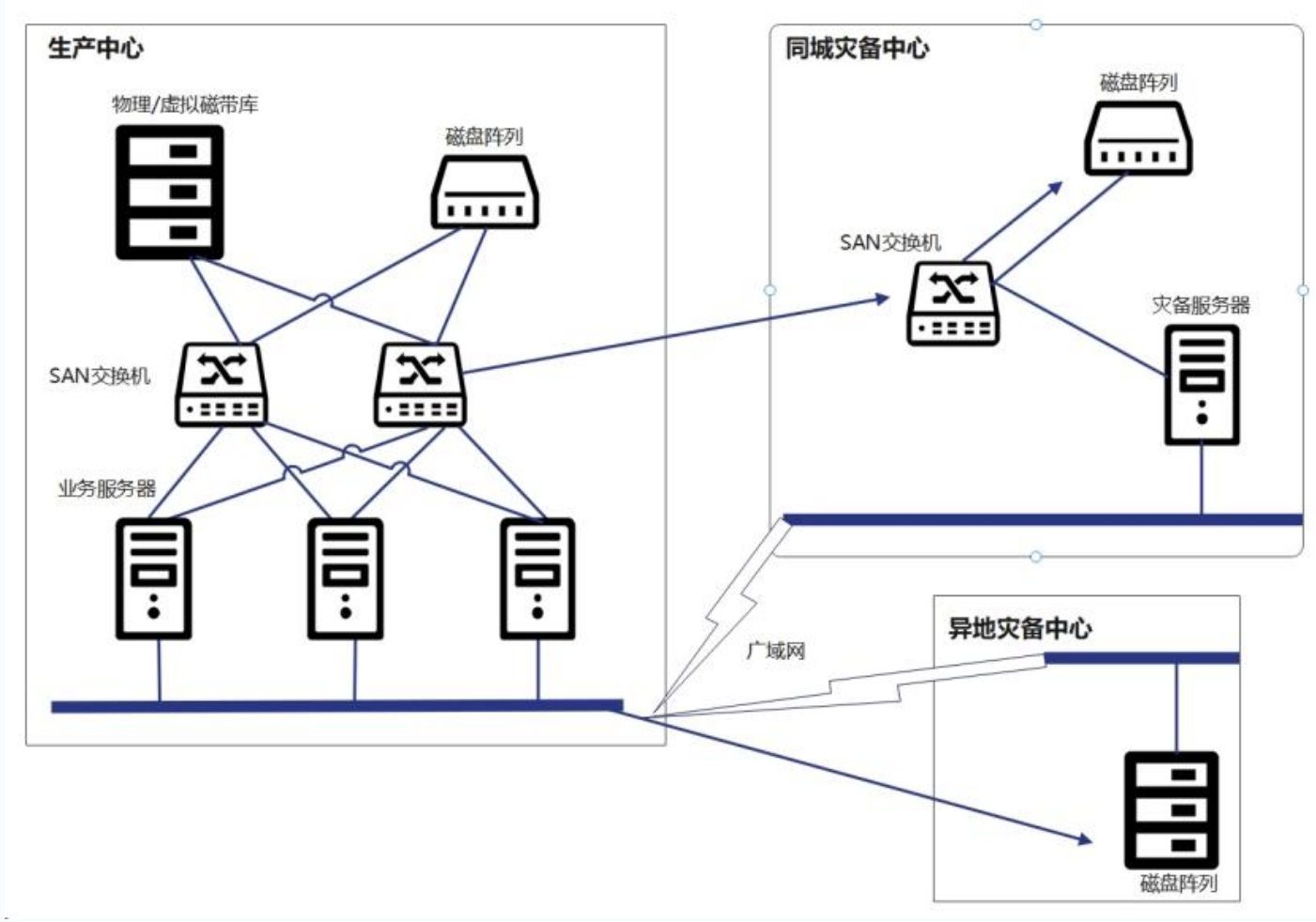
02 2.2.1 基于智能存储设备的数据复制技术

生产—同城及生产—异地（A—B及A—C模式）

在生产中心，数据不仅同步复制到同城的灾备中心，还通过广域网专线以异步方式复制到异地的灾备中心

复制过程如下：

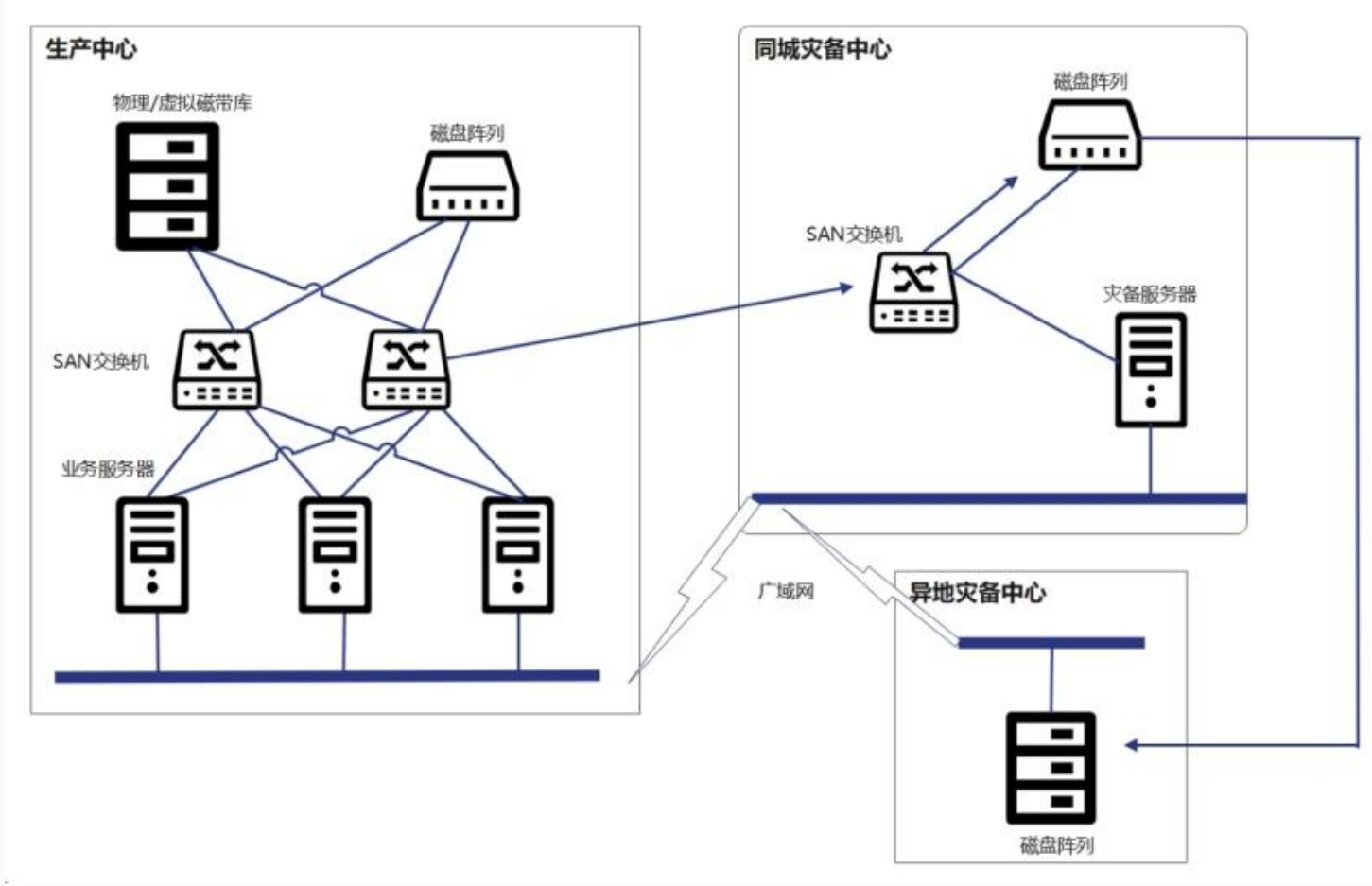
- 接收来自生产中心主机的写I/O操作
- 这些数据会被写入生产中心本地磁盘阵列的缓存中
- 向生产主机发送设备结束信号，表示数据已成功写入缓存
- 这些数据会通过特定的链路传送到同城灾备中心的磁盘阵列缓存中。一旦同城磁盘阵列接收到数据，它会向生产磁盘阵列发送数据接收确认信号，并修改磁道表，确保数据的完整性和一致性



02 2.2.1 基于智能存储设备的数据复制技术

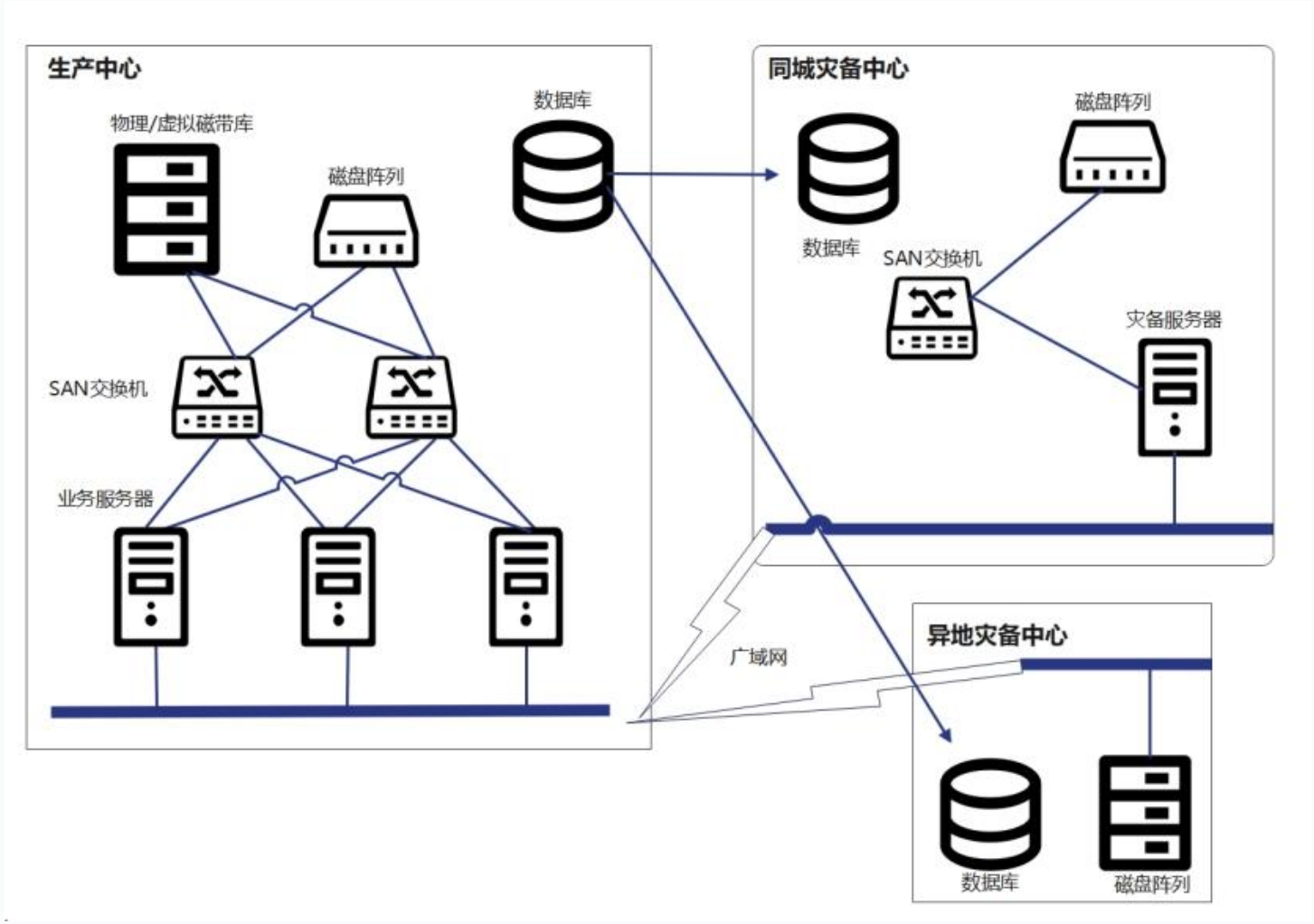
生产—同城—异地（A—B—C模式）

- 在数据复制过程中，生产中心首先将数据同步复制到同城灾备中心
- 同城灾备中心则通过广域网专线，采用异步的方式将数据进一步复制到异地灾备中心。
- 与直接由生产中心发起数据复制不同，这种模式下数据的复制过程是由同城灾备中心主动发起的。这种异步复制技术的主要优势在于，它对生产中心业务的正常运行影响较小



02 2.2.2 基于数据库的数据复制技术

- 基于数据库的数据复制技术通过使用数据库的日志备份与恢复功能，持续将归档日志或重做日志传输到灾备中心以实现数据同步
- 重做日志记录了事务对数据库的修改，而归档日志文件则保存了已完成的重做记录，对ORACLE数据库的备份和恢复至关重要。灾备中心利用这些日志文件进行数据恢复，确保数据的持久性
- 数据库同步软件的使用允许生产中心与灾备中心之间进行实时数据复制，支持不同级别的数据同步，包括整库级、用户级、表级和日志级，实现一对多模式的远程数据复制
- 数据库复制技术一般适用于应用级灾备模式

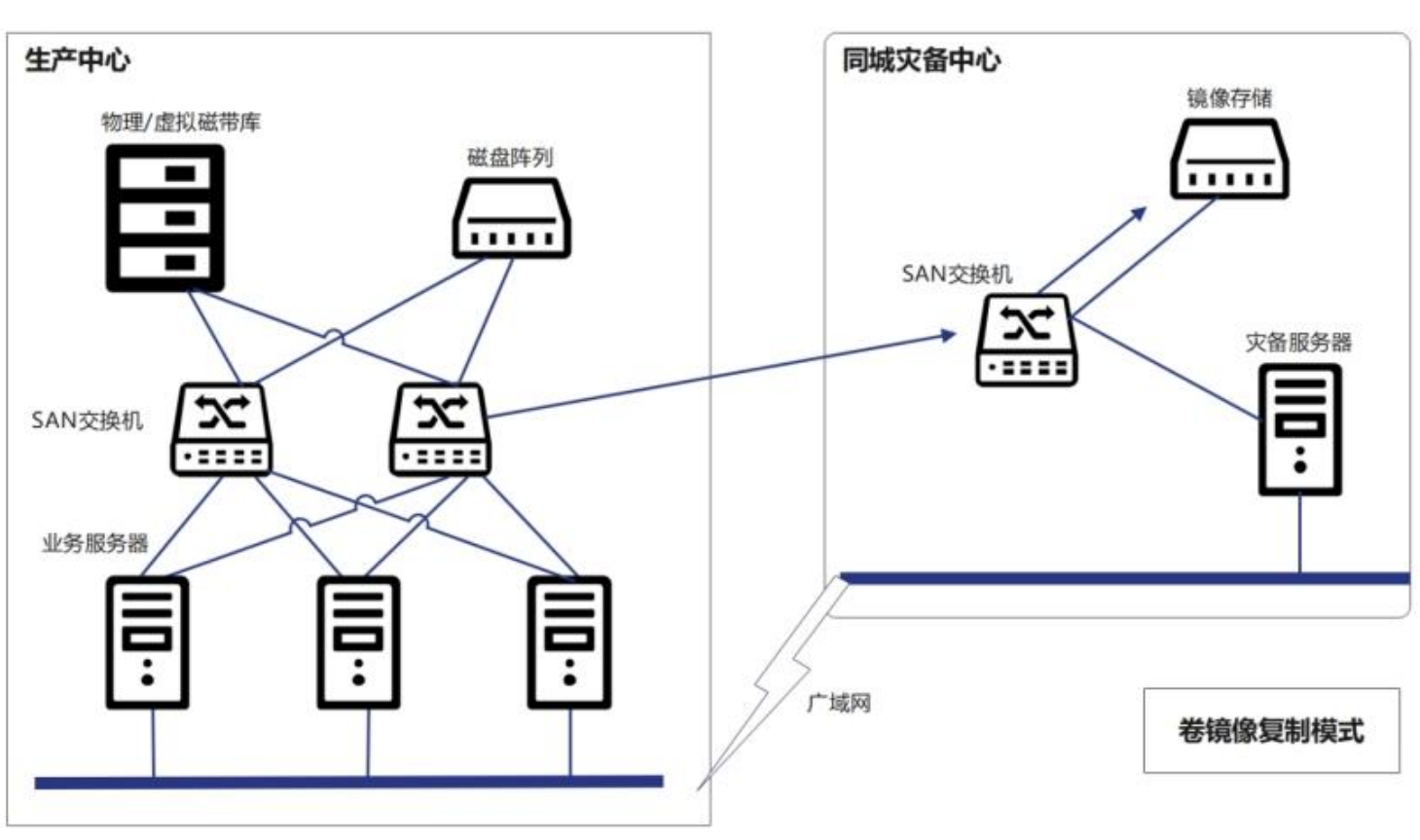


02 2.2.3 基于主机的数据复制技术（数据卷镜像方案）

数据卷镜像方案工作原理依赖于生产中心和灾备中心之间的光纤链路连接。在生产中心，所有需要进行数据复制的服务器上都会安装专业的存储管理软件。与此同时，灾备中心也会配备相应的存储系统和主机

数据卷镜像方案一

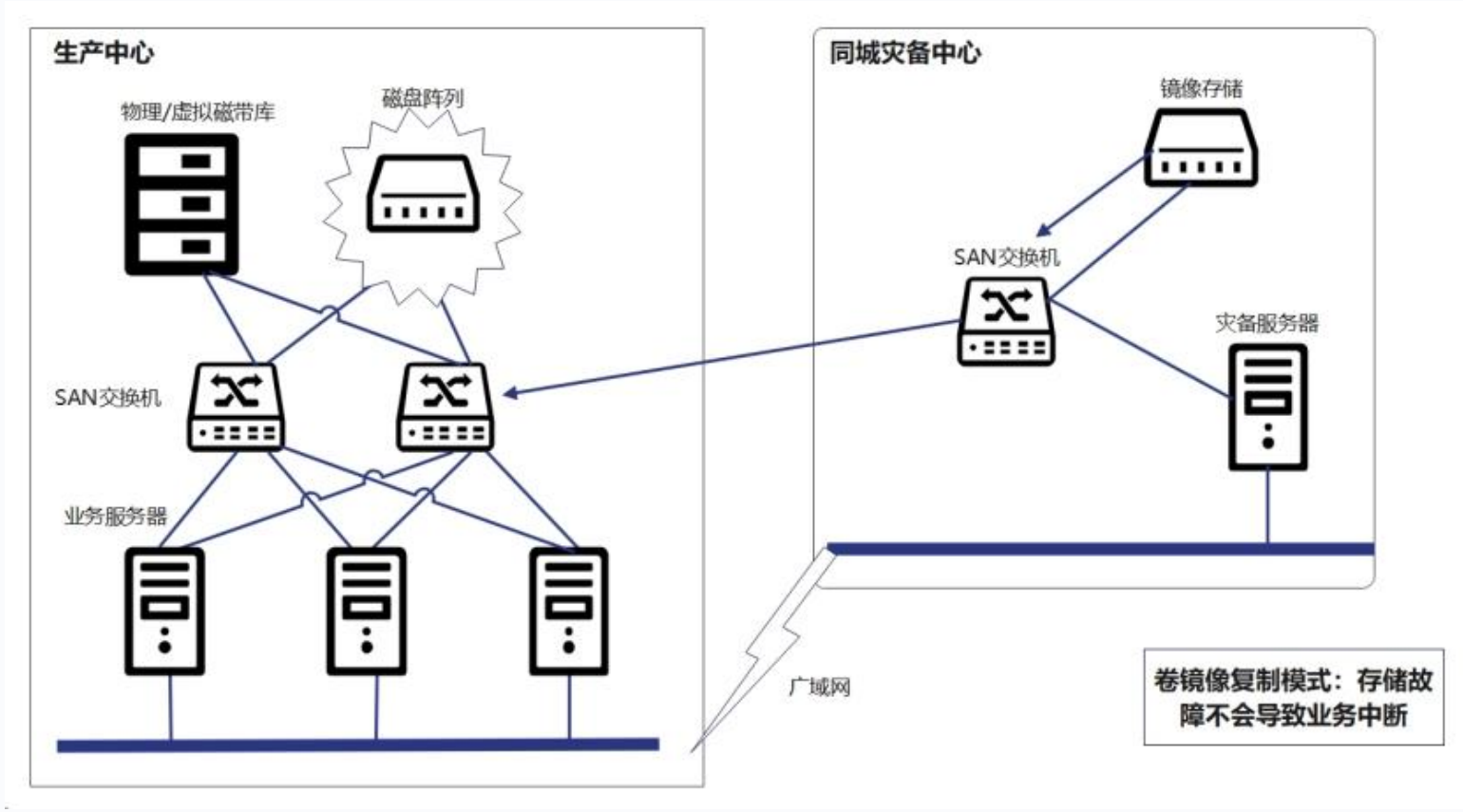
专业存储管理软件将生产中心和灾备中心的存储系统整合为镜像存储系统，实现数据同步。生产中心的写操作通过光纤链路实时传输至灾备中心，并在两地存储系统均完成写入后，操作才被视为成功。这种镜像方案确保了生产中心数据的"零丢失"，达到数据恢复点目标（RPO）为零



02 2.2.3 基于主机的数据复制技术（数据卷镜像方案）

数据卷镜像方案二

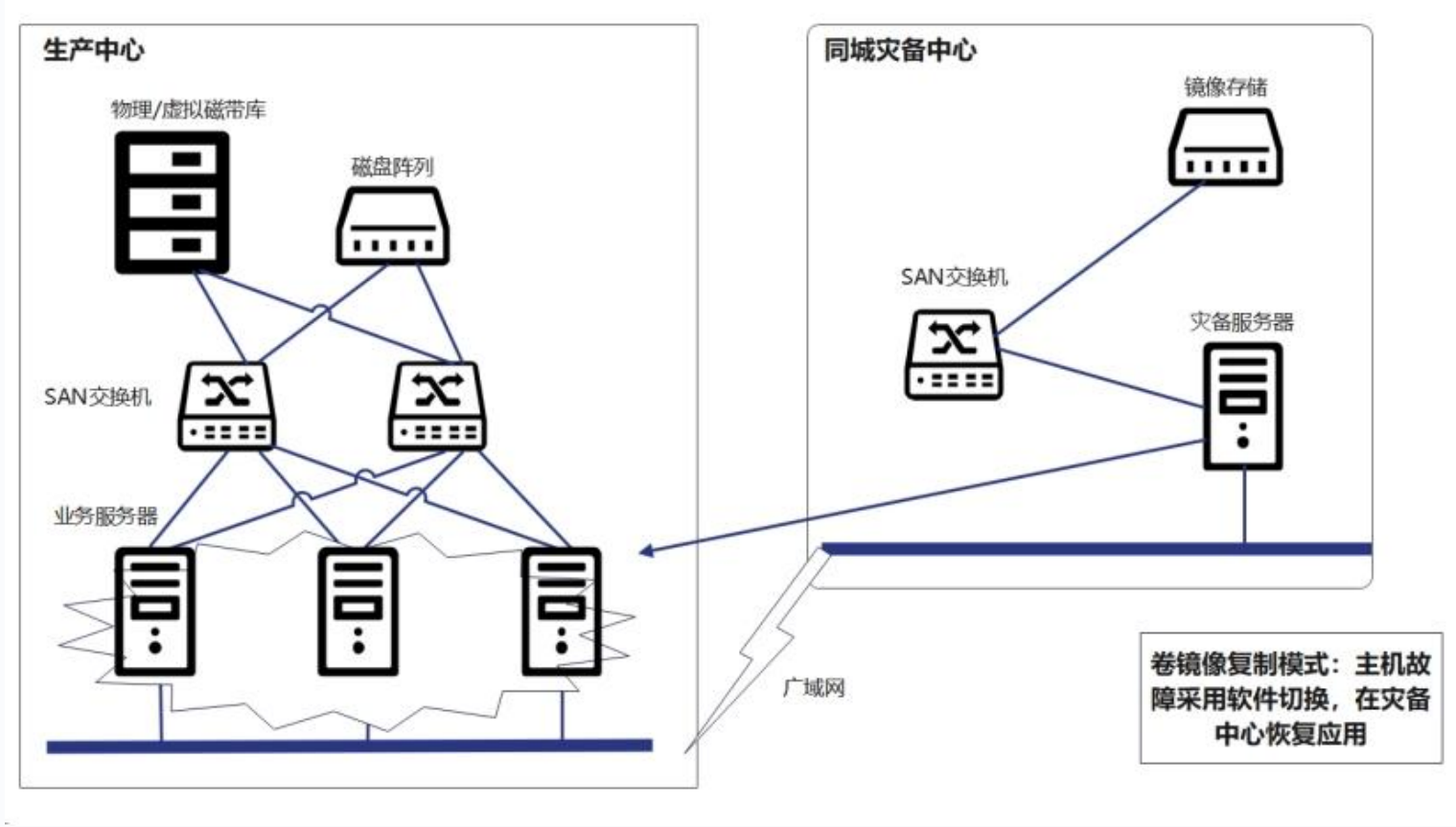
专业存储管理软件能够自动检测生产中心或灾备中心存储系统的故障，并迅速将其从镜像系统中移除。健康的存储系统将继续独立承担业务，保障业务连续性。在存储系统故障引发的灾难性事件中，软件自动执行灾难接管，无需人工干预，实现零恢复时间目标（RTO），即无停机时间



02 2.2.3 基于主机的数据复制技术（数据卷镜像方案）

数据卷镜像方案三

当生产中心的主机遭遇故障时，业务不可避免地会遭受中断。为了迅速恢复业务连续性，可以利用集群管理软件的灾难切换功能。这一功能能够在极短的时间内，自动将生产中心的应用无缝切换至灾备中心的主机上。通过这种自动化的切换过程，可以最大限度地减少业务中断的时间，确保业务的稳定运行

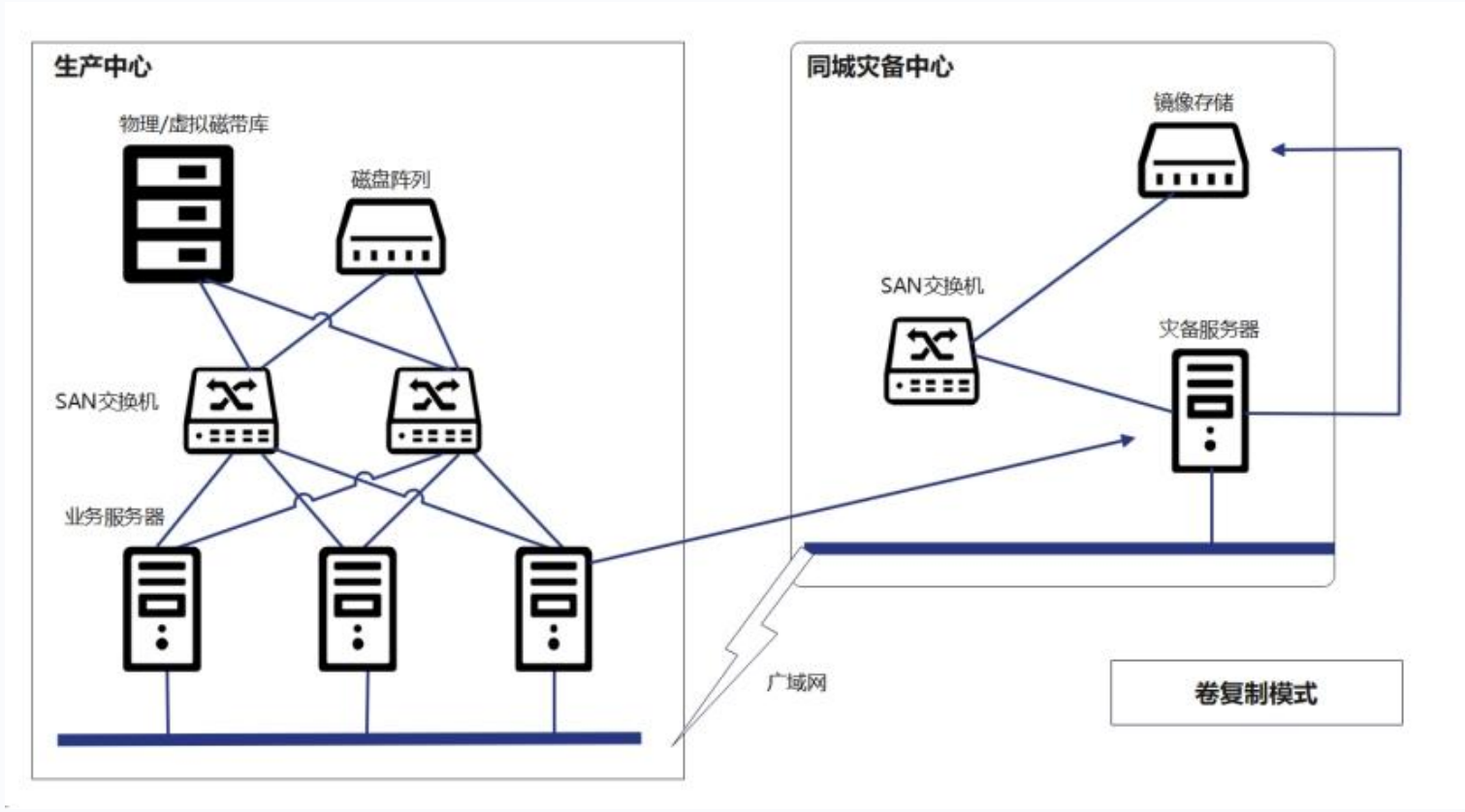


02 2.2.3 基于主机的数据复制技术（数据卷复制方案）

数据卷复制方案是一种基于主机的复制技术，依赖存储软件实现容灾数据复制，与数据卷镜像方案的主要区别在于使用IP网络代替光纤链路。它通常采用异步复制，允许灾备覆盖超远距离，不受距离限制

数据卷复制方案一

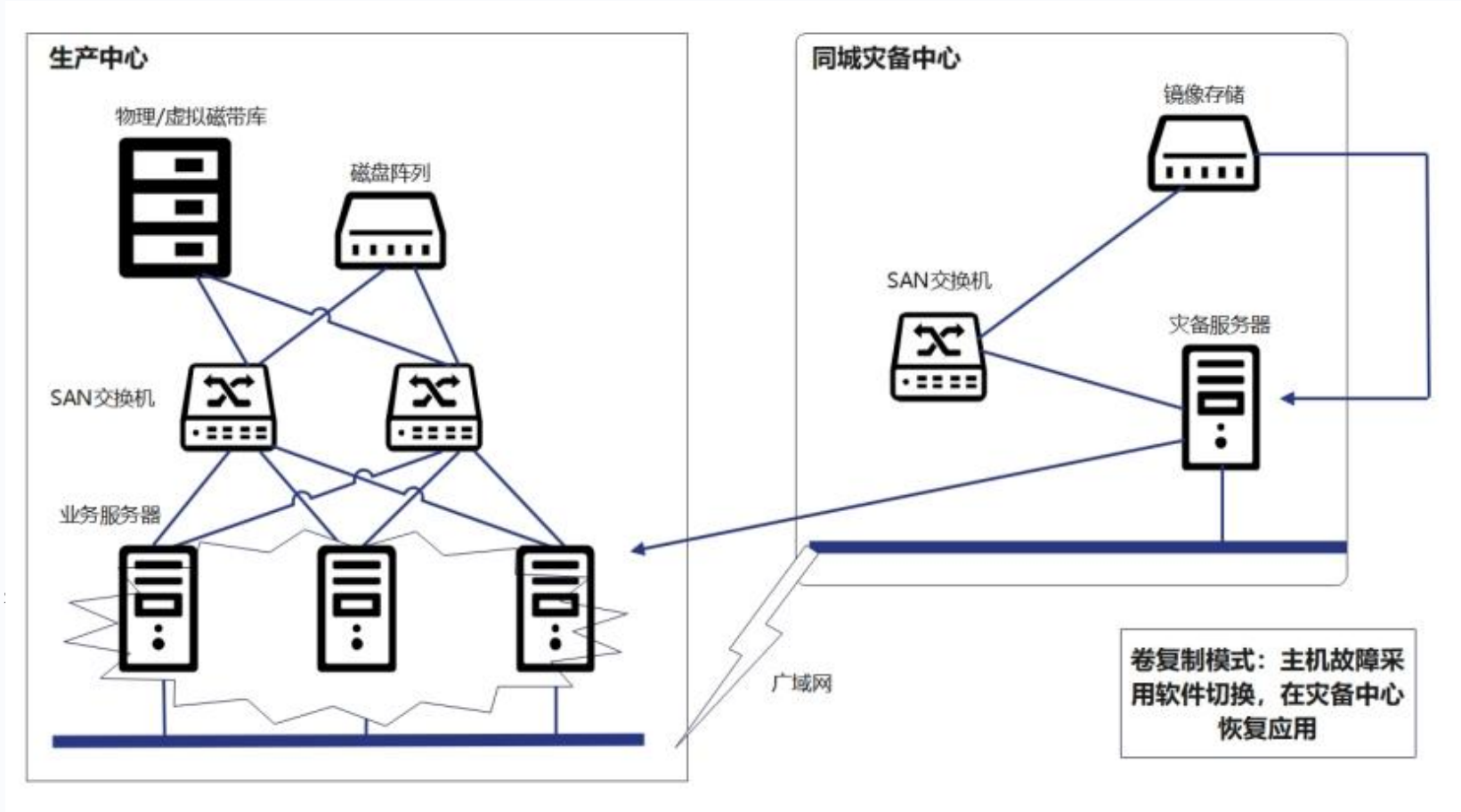
生产中心和灾备中心的服务器都需要安装专业存储管理软件，并设定相应的数据卷复制关系。一旦数据初始化完成，生产中心主机每接收一个写操作，都会同步通过IP链路传送给灾备中心的主机，后者则会在其存储系统上执行这一写操作



02 2.2.3 基于主机的数据复制技术（数据卷复制方案）

数据卷复制方案二

它支持高达32个逻辑数据卷对一个逻辑数据卷的复制功能，即支持多数据中心向一个灾备中心容灾的功能。无论是生产中心的主机还是存储器出现故障，业务都会暂时中断。此时，借助专业存储管理软件中的灾难切换功能，可以迅速将生产中心的应用自动切换至灾备中心的主机，这种切换过程能够最大限度地减少业务中断时间，保障业务的稳定运行

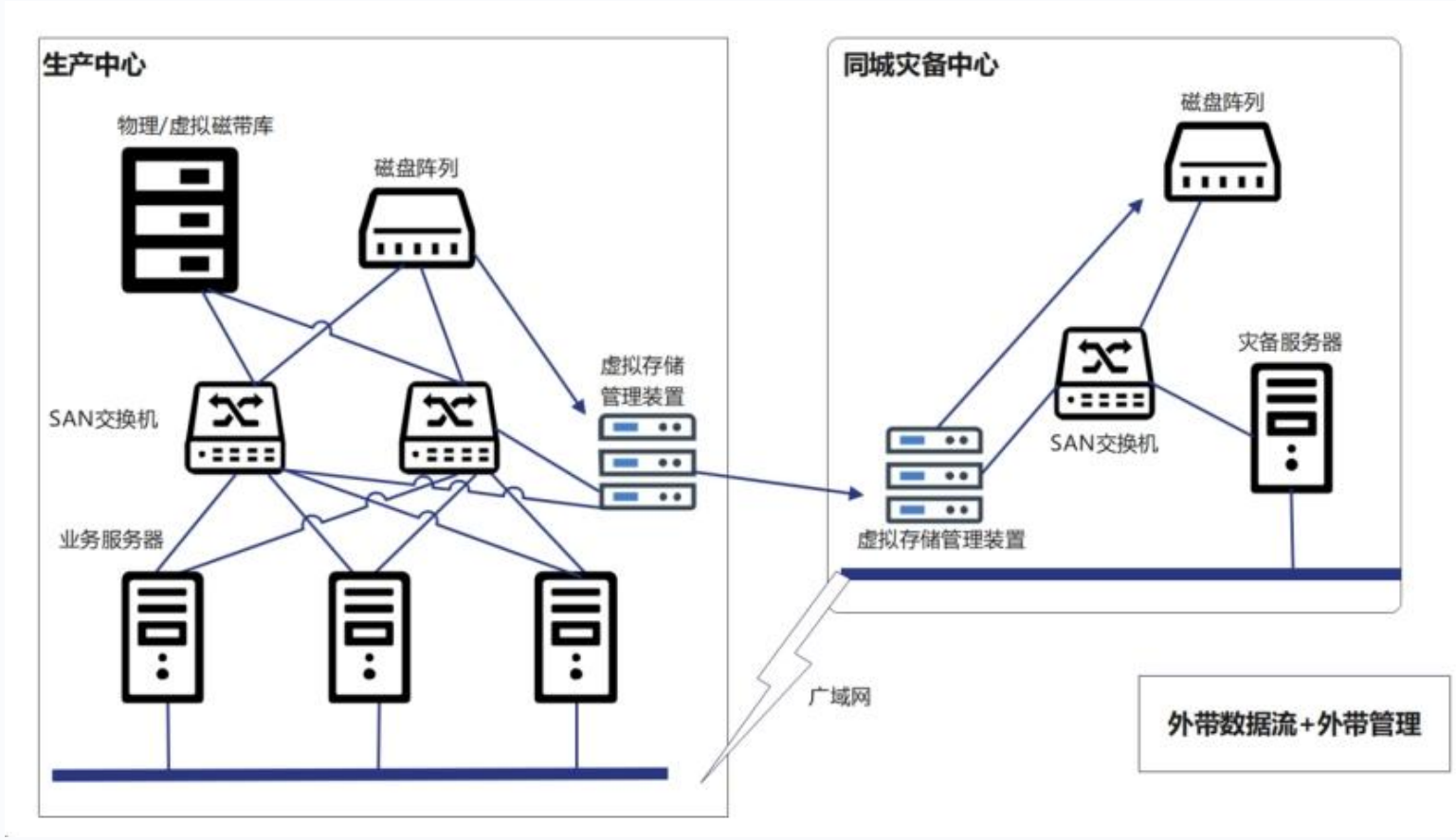


02 2.2.4 基于存储虚拟化的数据复制技术

虚拟存储技术通过集中管理多个存储介质，实现大容量和高速数据传输，同时分离物理存储与逻辑表示。存储虚拟化复制技术能够实现生产中心与灾备中心之间的逻辑卷复制，消除物理存储设备之间的差异。

模式一：带外数据、带外管理模式

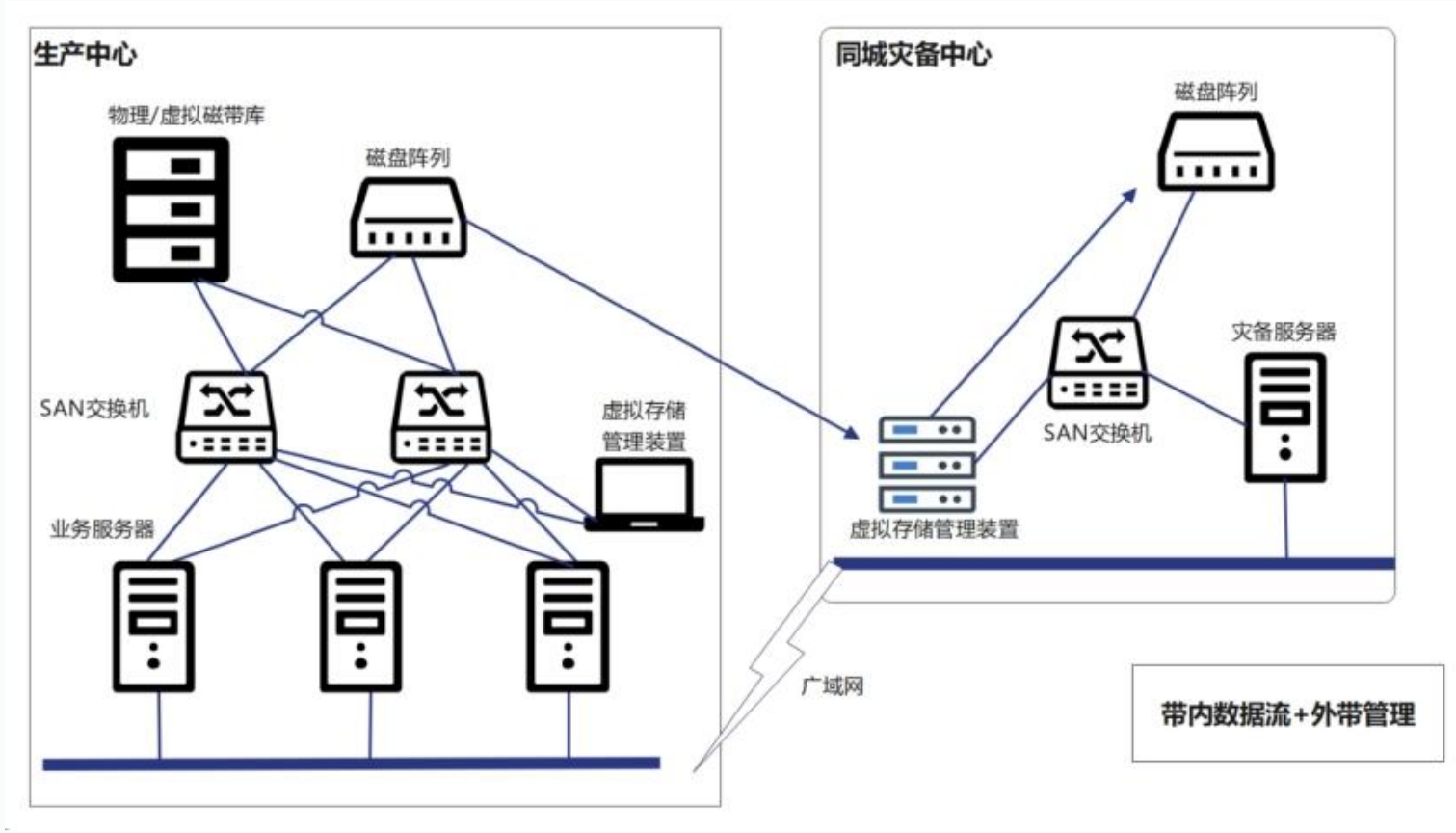
- 虚拟存储管理装置位于SAN网络旁侧通道，通过虚拟化端口对生产数据进行分割和捕获，并将操作记录到物理存储和本地虚拟存储设备
- 接收到的数据会被压缩打包，并通过SAN路由器的IP端口复制到灾备中心
- 虚拟存储管理装置的IP管理确保了装置故障时应用服务器对物理存储的访问不受影响
- 管理操作不影响生产系统性能，保障了数据高效复制和业务连续稳定



02 2.2.4 基于存储虚拟化的数据复制技术

模式二：带内数据、带外管理模式

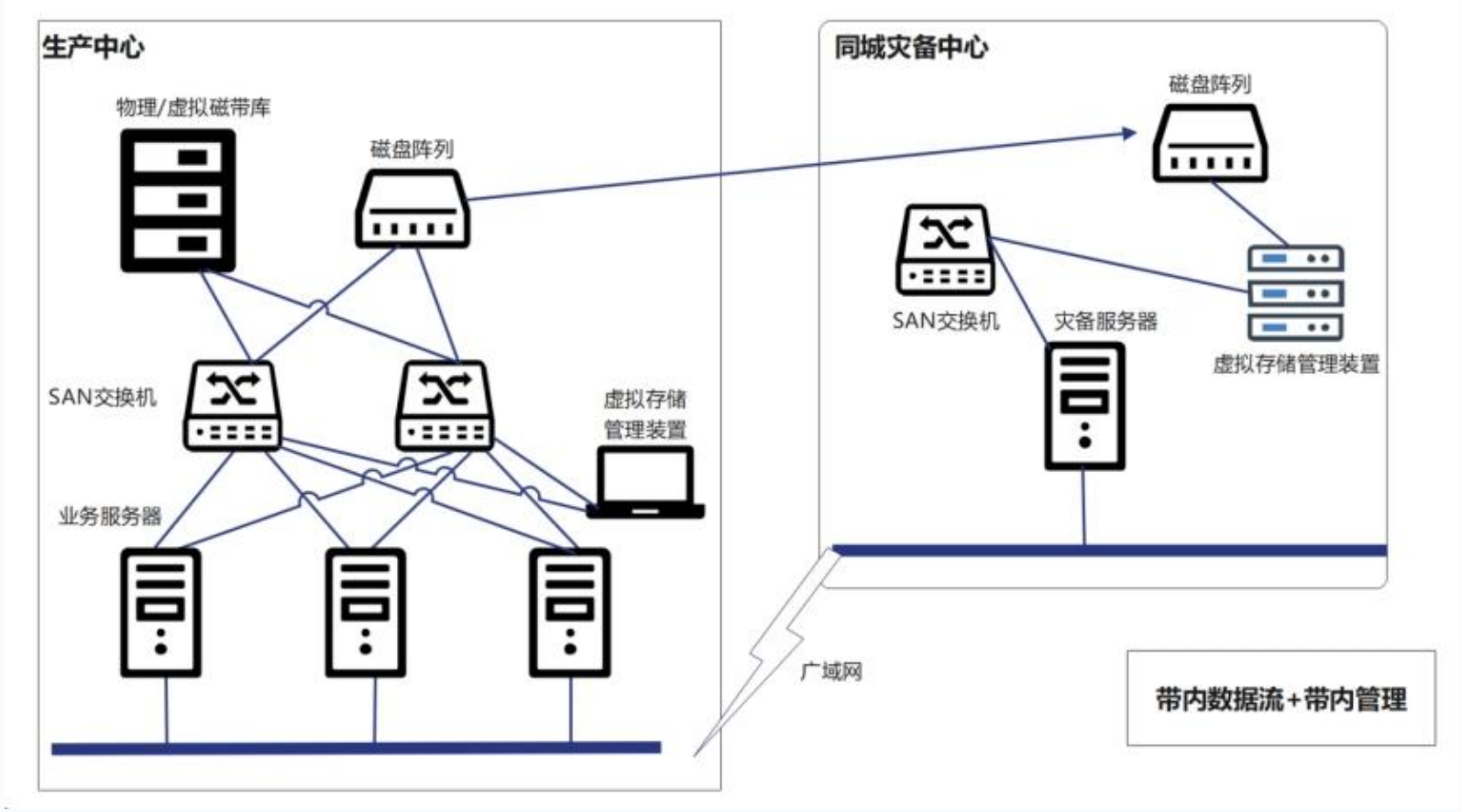
- 虚拟存储管理装置在SAN网络中充当应用服务器访问虚拟卷的中介，并负责将生产中心的逻辑卷实时镜像至灾备中心，以确保数据同步
- 管理操作通过IP进行
- 装置故障不会影响应用服务器对物理存储的访问
- 管理平台的操作不影响生产系统，确保了系统稳定性和数据安全性



02 2.2.4 基于存储虚拟化的数据复制技术

模式三：带内数据、带内管理模式

虚拟存储管理装置在SAN网络中是应用服务器访问虚拟卷的必经之路，同时负责生产中心与灾备中心的数据复制，但其故障可能影响生产业务。尽管如此，通过IP管理，即使装置故障，应用服务器仍可访问物理存储，且管理操作不影响生产系统性能。这种设计提高了系统的可用性和保障了数据安全。



02 2.3 灾备方案对比

- **基于存储虚拟化的数据复制技术**：特点是高效、灵活，能够集中管理和优化存储资源。适用于需要集中管理复杂存储需求的大型企业或数据中心，提供灵活的数据迁移和灾难恢复能力，对主机透明。

- **基于主机的数据复制技术**：特点是数据复制在主机层实现，通过软件或代理服务进行。适用于中小型企业或分布式系统，要求高性能和数据同步的环境，可以实现细粒度的数据管理，但可能占用更多主机资源。

- **基于智能存储设备的数据复制技术**：特点是自动复制和同步数据，内置于智能存储设备中，无需额外软硬件。**适用于对数据可用性和业务连续性要求极高的关键应用**，如金融、电信行业，提供高性能和稳定性。

- **基于数据库的数据复制技术**：特点是专门针对数据库数据进行复制，确保数据的一致性和完整性。适用于数据库密集型应用，如*OLTP*或数据仓库系统，需要确保数据一致性和完整性的场景，以及需要多点或多级复制的业务。

第1章 数据安全概述

本讲内容概要：

01 第一节—数据容灾备份概述

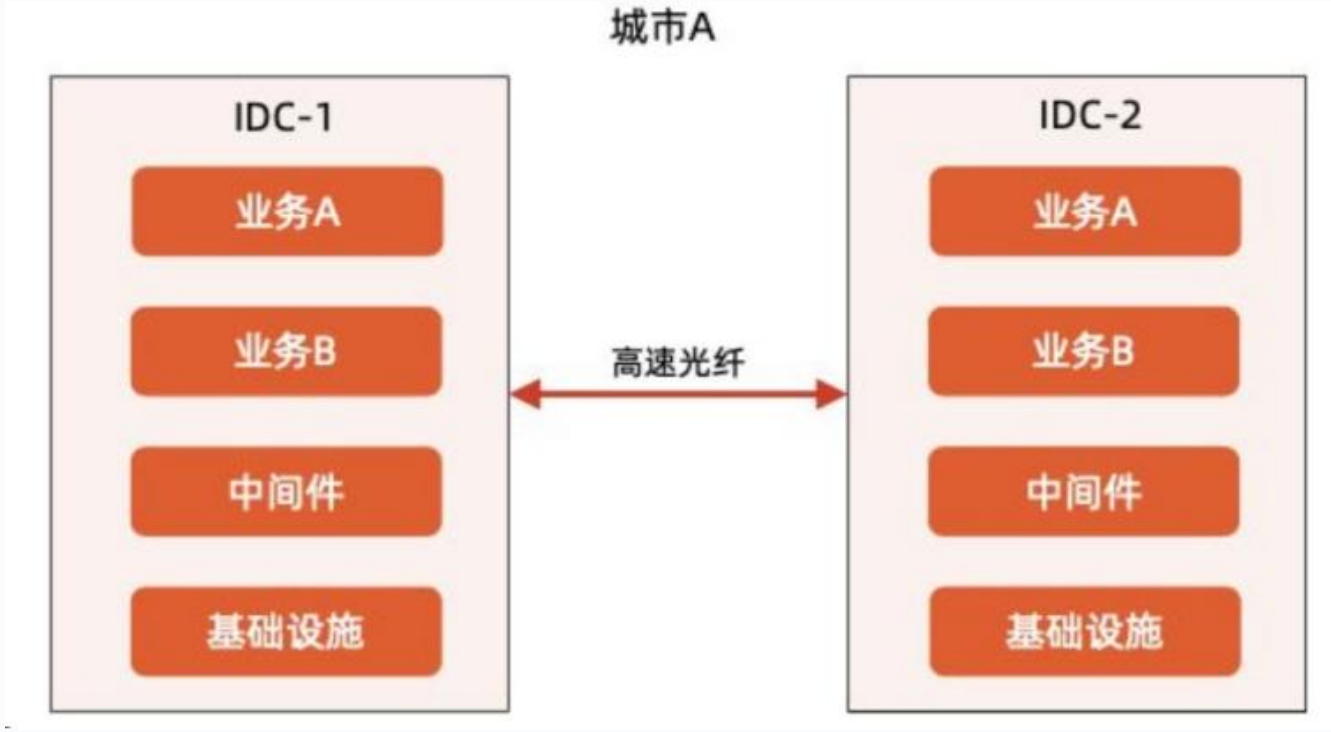
02 第二节—数据容灾备份技术

03 第三节—容灾备份系统的构建

03 3.1双活

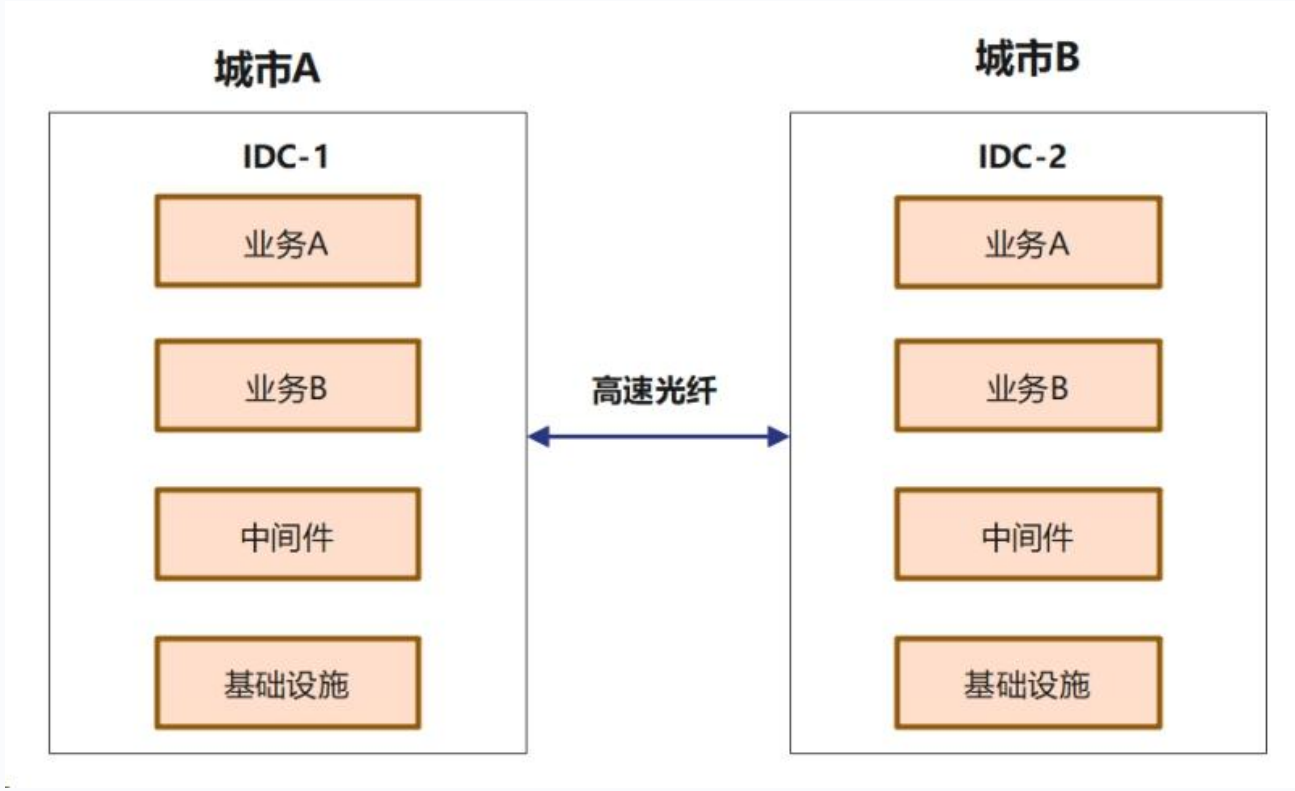
- 双活是指在两个生产中心部署相同的两个能力相同的业务系统
- 两个系统同时工作，地位对等、不分主从。具备在对方系统灾难发生时，接管对方业务的能力
- 双活通常需要负载均衡技术的支持

03 3.1.1 同城双活



- 同城双活模式是指在同一个城市内建立两个机房，它们各自承担一部分流量，一般入口流量完全随机，内部RPC（Remote Procedure Call）调用尽量通过就近路由闭环在同机房
- 这种模式旨在保证服务的高可用性，当一个机房不可用时，另一个机房能够单独对外提供完整的服务
- 核心优势在于，同城内的两个机房距离比较近，通信线路质量较好，比较容易实现数据的同步复制，保证高度的数据完整性和数据零丢失

03 3.1.2 异地双活



- 异地双活模式是一种高可用性分布式系统架构，通过在不同城市设立独立机房来确保业务连续性
- 机房分布在不同的地理位置，即使面临自然灾害也能保证至少有一个机房能够继续提供服务，大大降低了单点故障的风险，异地双活模式的机房能够通过高速网络和数据复制技术保持数据的完整性和一致性
- 该模式能够在机房故障时迅速切换至正常运行的机房，保障服务的可用性和业务的连续性

03 3.2 灾备

- 灾备是指具有主从之分的灾备系统（双活是不分主从的灾备）
- 通常是建立一个主业务系统和一个从属（备用）的业务系统（可能只有数据中心），正常情况下仅有主业务系统在工作，在主业务系统故障时，在启用备用系统
- 灾备有**热备、冷备**等方式

03 3.2.2 热备

热备是一种实时或准实时的数据备份策略，确保在主系统故障时能迅速切换至备份系统，最小化业务中断

热备通常用于关键业务系统，以确保数据的高可用性和业务连续性

热备具有实时同步、快速切换、零数据丢失、持续可用性的特点

03 3.2.1 冷备

冷备是一种数据备份策略，备份系统不与主系统实时同步，而是按计划周期性地进行数据备份

冷备适用于不需要实时数据同步的场景，主要用于灾难恢复，备份可以是全量、增量或差异形式

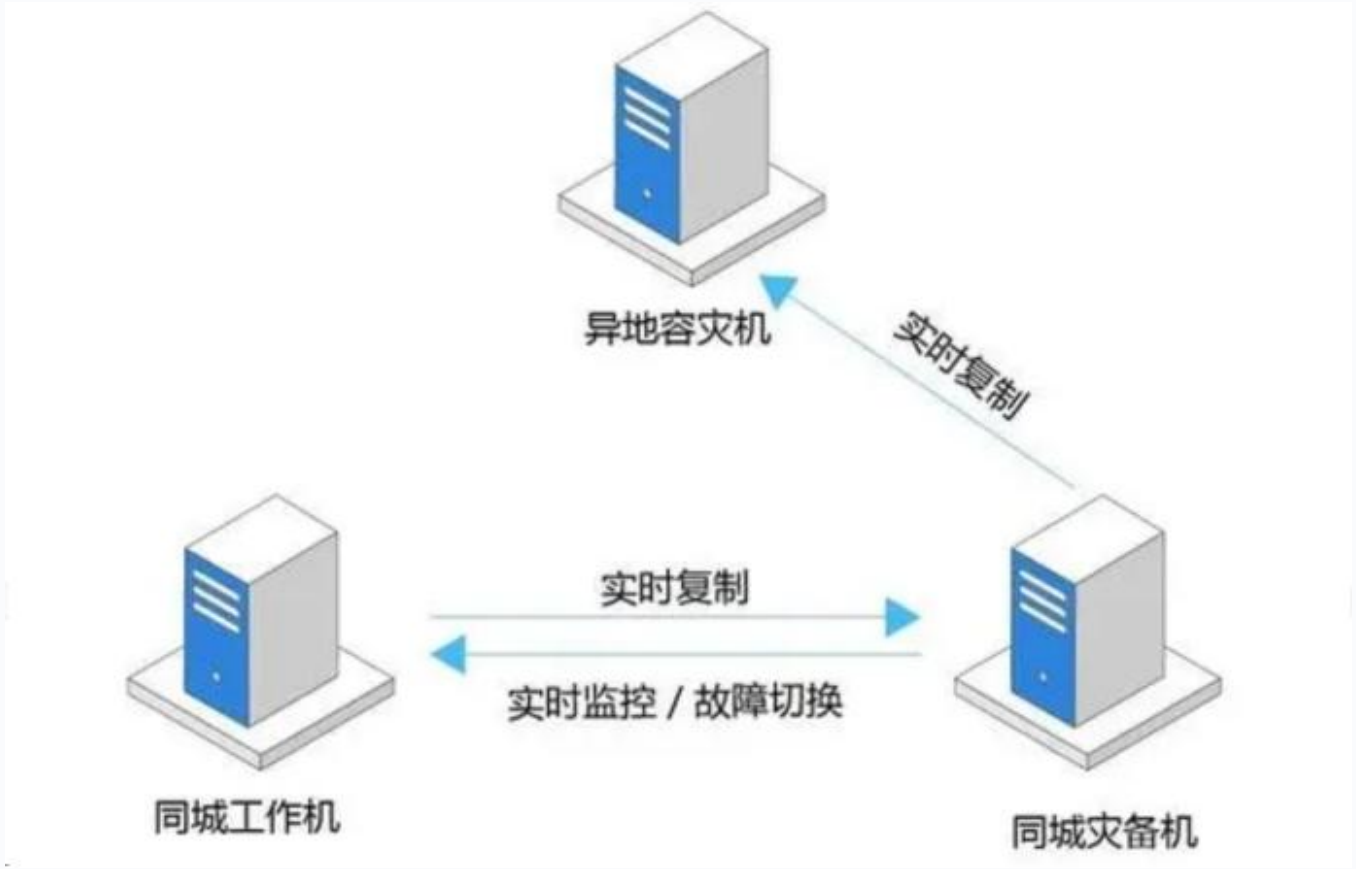
冷备在主系统故障时恢复数据和系统启动需要时间，可能导致服务中断，但有助于优化资源使用和减少对生产系统的影响

03 3.3 两地三中心

- 定义：两地三中心是一种企业级的数据备份和灾难恢复策略，通过在两个不同地理位置设立一个主生产中心和两个备份中心来提高业务连续性和数据安全性。该架构允许主生产中心的数据通过定期或实时同步到备份中心，确保数据的多份拷贝和高可用性

- 意义：在灾难情况下，两地三中心架构能够实现快速切换，从而最小化业务中断和数据丢失

03 3.3 两地三中心



谢谢！